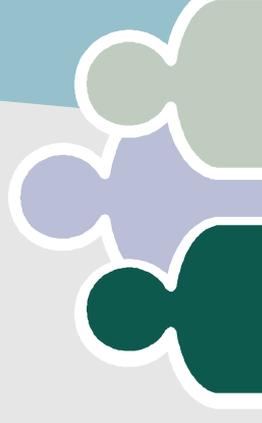


Computer Security

Transition Briefing
CD Head
22 October, 2002



Introduction

CS thru the ages @ FNAL
Threat Environment
Strong Authentication
CD Responsibilities
Projects and Forecast
Wrapup and Discussion



Overall Philosophy

- **Open Scientific Inquiry**
 - “Scientific thinking and innovation flourish best where people are allowed to communicate as much as possible unhampered.”
Enrico Fermi Dec 2, 1952
- **Responsible Control of Resources**
 - Who gets access to resources
 - Focus on this aspect
 - What they (can) do with them
 - Allow maximal freedom here
- **Zero Tolerance doesn't belong here**
 - Striving for zero incidents is too costly for the risk involved.



History

- **DOE Liaison - CPPM period**
 - (pre 1997) Lab had to identify role to satisfy DOE requirements but took no organized action against incidents.
- **FCIRT period**
 - (1997 – 1998) Focus was on response by expert SWAT team.
- **SysAdmin period**
 - (1998-2001) Focus on system hardening
 - Strong Authentication
 - Linux AutoRPM



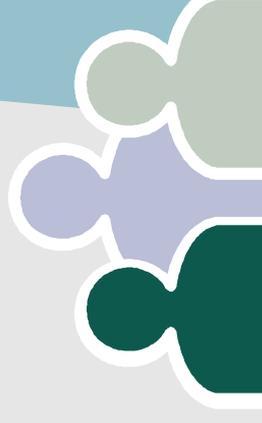
History (cont'd)

- Monitoring period
 - (2001 - current) Active scanning site looking for vulnerable and non-compliant systems
 - Active monitoring of traffic for threatening and non-compliant activity



In Our Little Town ...

- The Fire Department
- The Building Code
- The Police Department
- Customs and Passport Control



The Fire Department

- **FCIRT**
 - The initial focus was on a highly skilled SWAT team approach to respond and resolve incidents themselves.
 - Scope and number of incidents outgrew this approach by '98
 - Still mainstay of program and highly effective/respected.
- **Incidents**
 - **FIRE – Fermi Incident Response Emergency**
 - High level threat of damage or exposure to embarrassment
 - **SMOK – System Manager Okurance**
 - Single system threat or configuration error
- **Tools**
 - High level human intelligence
 - Network flow information



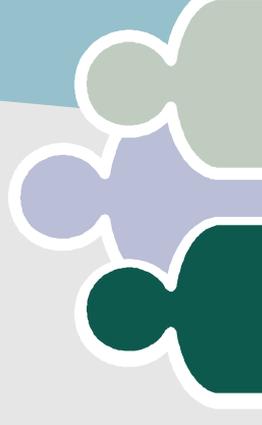
The Building Code

- **Strong Rules**
 - Give simple list of key rules and expect conformance
 - Implies “hang a few admirals” approach
 - Ignorance of the law is a common excuse
 - **Education**
 - Self help lists and meetings among peers in the trenches
 - Recommended practices collected
 - Some formal training programs (Linux admin, Strong Auth)
 - **Configuration Management**
 - AutoRPM for Linux hugely successful
 - Windows patch service and centralized virus scanners
 - **Strong Authentication**
 - Reduce threat of password compromise

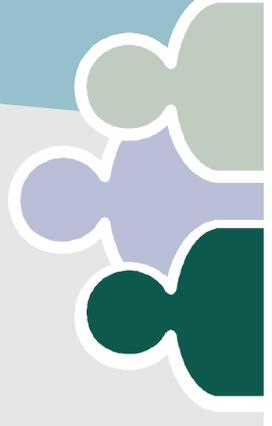
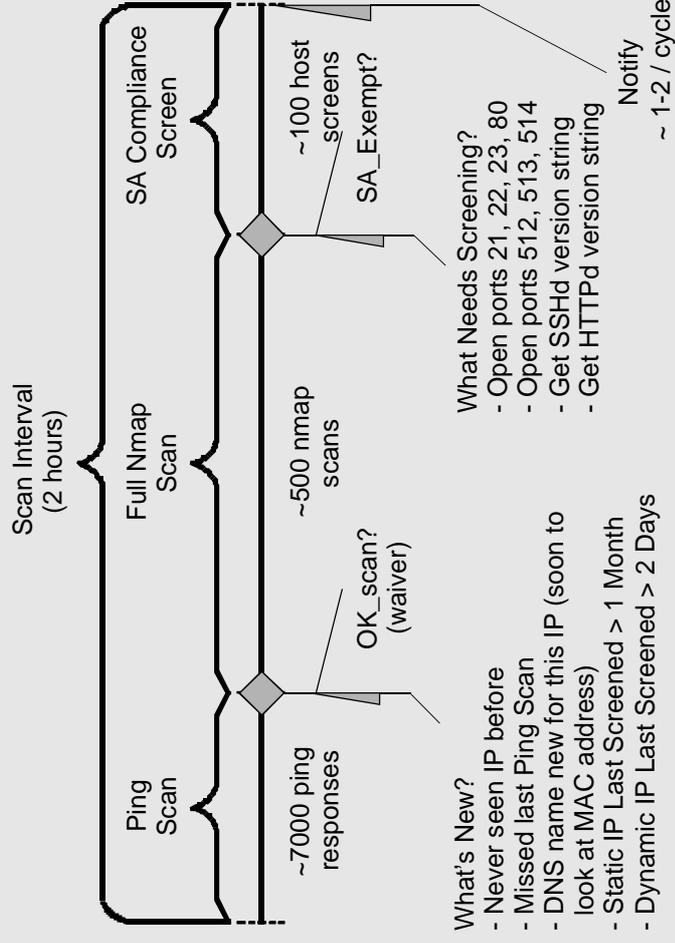


The Police Department

- Scanning
 - Preconfigured tools too heavy handed and coarse
 - Strong Authentication rollout tool
 - Vital for dealing with SSH vulnerabilities Oct-Dec 01
 - Useful ongoing tool for proactively dealing with new vulnerabilities
- Strong Rules Enforcement
 - Monitor for system configuration
 - Monitor for exposed passwords
- Self Assessment
 - Critical System reviews
 - Operational Readiness Reviews

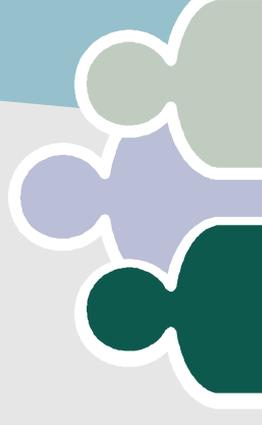


Scanner



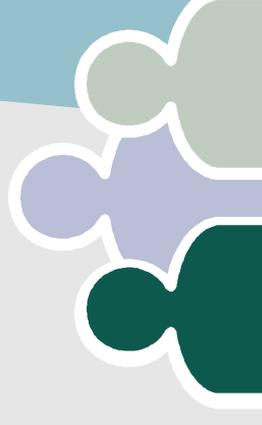
Passport Control and Customs

- The GRID



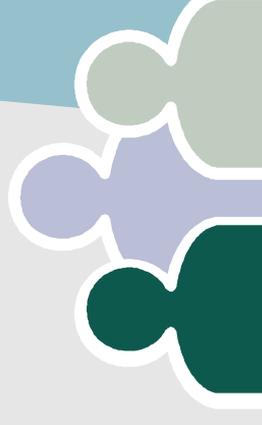
Threat Environment

- The Lab is under continual probe by:
 - Worms (programs that spread by self initiation)
 - Scans (programs that look for configuration info)
 - Attack scripts (programs that try to exploit an application hole for purpose of running some other application)
- The Lab is an attractive target:
 - We have very good network connectivity
 - There are a lot of machines of different type
 - We are a .gov facility



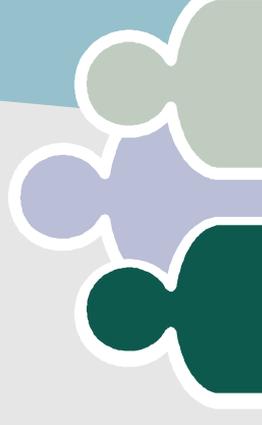
Threat Environment II

- Once a program is installed on a machine, one has little control over what actions it may take.
 - We've had no instances of premeditated damage
 - We've had few instances of direct damage



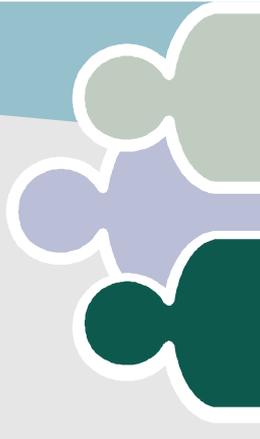
Risk Analysis

- Institutional Risk
 - Data, or the ability to take data, might be destroyed
 - Largely a data protection issue
 - The ability to operate the facility might be disrupted
 - This is covered by stand alone operations, border defenses, disaster recovery plans
 - Confidential Data might be exposed
 - With few exceptions largely and issue up to data owners
 - Some data has legal
 -



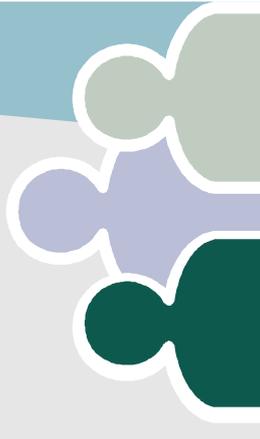
Risk Analysis (cont'd)

- Franchise Risk
 - Our sponsors may withhold our franchise to operate if they lose faith in our abilities.
 - The general public may insist on protection from misuse of publicly funded resources.
 - We may lose reputation through miscommunication or inflation of low level incidents.
 - We may be used as a “firebase” and incur liability.



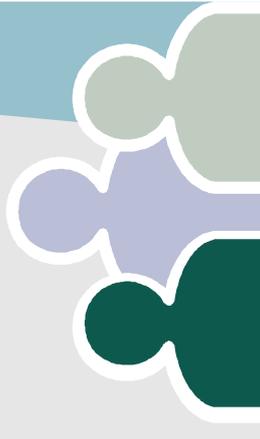
Strong Authentication - Origin

- Motivations
 - A number of very costly system intrusions which exploited stolen passwords and other weak authentication, such as .rhosts files.
 - Poor understanding of who has, and who should have access.
 - Mandate
 - Reduce such intrusions by 90% or better.
 - Demonstrate affirmative control over access to Fermilab computing facilities.
 - Methods Considered
 - Tight perimeter controls.
 - Requiring encrypted sessions.
 - Strong, centralized authentication.
- ⇒ Kerberos v5



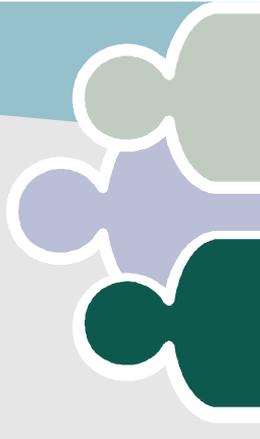
Strong Authentication - Status

- All* systems are required to accept only Kerberos tickets or challenge-response authentication tied to Kerberos for remote login, shell and ftp access.
- Compliance is near 100% for Unix, coming along in Windows.
- Illicit system access through stolen passwords has not occurred on any compliant system.
- (Stolen mail server passwords have been used.)
- * Waivers are available when justified.
- Maintenance effort is low.
- Kerberos accounts are created and terminated through CNAS for both the Unix-based realm and the Windows realm.
- Password requests handled by CD office for Unix-based realm, by OU admins in Windows.
- Software maintenance effort < 0.1 FTE.



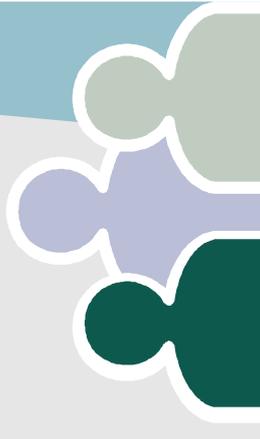
Collateral Benefits of Strong Auth.

- Integration of Unix and Windows authentication.
- A solid security infrastructure for other network applications (cvs, rootd, ldap, fbs, lsf, sam).
- Single-signon secure email (IMAP pilot in BD).
- Windows application security through IPsec.
- Central login auditing.
- Improvements in system-to-user association.
- Tested, but not yet widely used:
 - Grid PK credentials on demand.
 - Web PK credentials on demand.
 - Cross-cell AFS authorization.



CSPP Roles & Responsibilities

- Computer Security Executive (CSExec)- Nash/Skow
 - Delegated by Director
- Computer Security Coordinator (FCSC) - Crawford
 - Reports to CSExec on computer security.
 - Principal computer security manager for the laboratory.
 - Chief point of contact for external organizations (CIAC, FBI, etc.)
 - Deputies: Gaines, Education; Dyxin, Government Liaison.
- FCIRT Head - Petravick
 - Reports to CSExec during an incident, to FCSC at other times.
 - Deputy: Kaletka
 - Not a CD function *de jure*, but it rests heavily on CD.
- Computer Security Working Group (CSWG)
 - Advises CSExec and FCSC; chaired by FCSC.
 - Broad but CD-heavy membership.



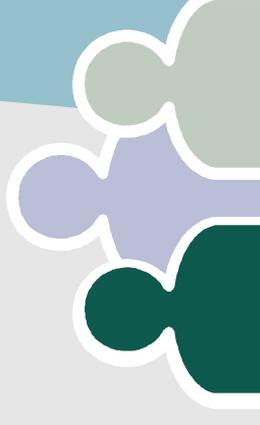
More Security Roles

- Critical System Coordinators
 - Authentication Infrastructure, Core Network, BD Controls, BSS, CDF Online, D0 Online.
 - Next: Buildings Controls.
- General Computer Security Coordinators (GCSCs)
 - One for each division, section and major experiment.
 - Appointed by div/sec head or spokesperson as part of Integrated Cyber Security Management.
 - Resource to div/sec/exp, FCSC and FCIRT.
 - CDF, D0 and FESS have a CD person as GCSC.



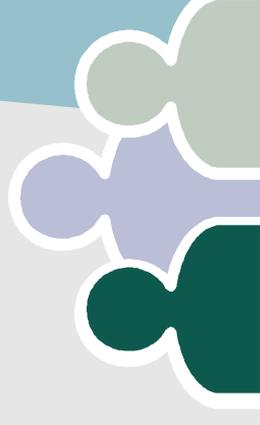
Computer Security Team

- Full-time: Crawford, Reitz.
- Partial: Dyxin, Gaines, Kaletka, Skow, Petravick.
- Ongoing activities
 - Monitoring and evaluating new vulnerabilities and threats.
 - Scanning F2AL systems to find problems before the bad guys.
 - Maintaining Kerberos infrastructure.
 - Advising users, admins, engineers, developers.
 - Participating in standards development.
 - Educational program.
 - Incident response.
 - Responding to outside reports, reporting to outside entities.



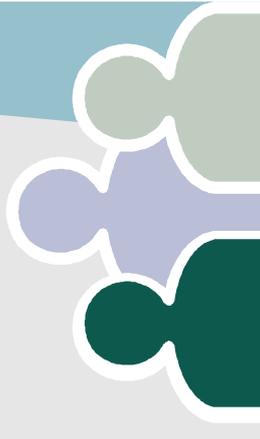
Future Directions

- Our weak areas are
 - Configuration management (OS & application versions, patches).
 - Remaining cleartext authentication in various protocols.
 - The ease with which new, vulnerable services are deployed.
 - Asset location and responsibility.
- Threats on the rise
 - Rapidly propagating worms and viruses.
 - Windows SMB, RPC and CIFS attacks.
 - Man-in-the-middle attacks against session encryption.
- Expected future threats include
 - Connection hijacking.
 - Attacks on DNS and routing.
 - Automated exploit generators.



Future Developments

- **Musts**
 - Inter-site trust - in some form or another.
 - Rationalized PKI.
 - A safer public network, including
 - Mandatory system registration for use of wireless and wall jacks.
 - Tiered network architecture site-wide.
- **Shoulds**
 - Better accountability for systems on the network.
 - Eliminate remaining weak authentication.
- **Mays**
 - Ubiquitous packet-level authentication.



Overview of Exemptions from Strong Authentication Policy

- By Division:
- PPD - 8
 - LSS - 6
 - BSS - 1
 - TD - 10
 - Dir - 3
 - FESS - 12
 - CD - 26
 - D0 - 5
 - CDF - 4
 - Beams - 50
 - Total - 125

Type:

- Timbuktu or other file shares or remote execution on PCs: 60
- terminal server, WinCenter : 3
- PC ftp servers: 3
- Proprietary vendor SW 10: 7 (backup), 1 (SGI SW install), 1 (Data OnTap) 1 mosix
- Legacy Systems 16: 6 VMS, 4 IRIX, 1 Linux, 3 SUN, 1HP, 1 AIX
- Private networks (VxWorks, etc): 20
- Other 14



Summary of users exposing Kerberos passwords

count of unique USERS by week and by division/section/experiment

WEEK #USERS CD CDF D0 BD MISC PPD

Aug 19	12	1	5	6	0	0	0
Aug 26	37	4	22	11	0	0	0
Sep 02	38	5	18	11	0	2	2
Sep 09	21	6	9	2	0	4	0
Sep 16	22	3	10	5	1	1	2
Sep 23	19	2	9	7	0	0	1
Sep 30	16	2	7	5	0	0	2
Oct 07	11	1	7	2	0	0	1
Oct 14	12	2	3	5	1	1	0
Oct 21	4	0	1	3	0	0	0
Total	144	21	64	41	2	8	8

17 users have received
level 2 warning

(CD includes all logins to CD machines)



Summary

- Computer Security is a Labwide responsibility, but CD must take a leadership role.
- Our particular responsibility is for actions involving our site, but our operational scope is the global community of scientists.

